

NEWPORT GIRLS' HIGH SCHOOL ACADEMY TRUST



ONLINE SAFETY POLICY

Policy written by: Designated Safeguarding Lead

Policy written/reviewed: Summer 2026

Next review due: By the end of Summer Term 2028

Statutory Trustee Approval:

I. Statement of Intent

Newport Girls' High School is committed to providing a safe, secure and inclusive learning environment where all members of our community can benefit from technology whilst understanding how to use it safely, responsibly and respectfully.

Online safety is recognised as a fundamental safeguarding responsibility. Digital technologies are embedded throughout education and everyday life, providing significant opportunities for learning, communication and creativity. Alongside these opportunities come increasingly complex safeguarding risks. Our approach reflects the understanding that safeguarding children today requires schools to protect students both offline and online.

The school recognises that online risks continually evolve. Children may be exposed to harmful or illegal content, manipulated through online contact, encouraged towards harmful behaviours, exploited financially, or subjected to abuse through emerging technologies including artificial intelligence. Newport Girls' High School therefore adopts a proactive approach which develops students' digital resilience alongside robust safeguarding systems.

Our online safety strategy is based upon four key principles:

- safeguarding all members of the school community
- educating students to become responsible digital citizens
- maintaining effective filtering and monitoring systems
- responding promptly and proportionately to concerns.

Online safety is not viewed as a standalone subject. It is embedded throughout safeguarding, behaviour, pastoral care, curriculum delivery, staff training and leadership.

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- ICT Acceptable Use Agreements
- Data Protection Policy
- Searching, Screening and Confiscation procedures
- Mobile Phone and Personal Electronic Device Procedures
- Relationships, Sex and Health Education Policy
- Anti-Bullying Policy

2. Legislative Framework

This policy has been developed in accordance with current statutory legislation and guidance including:

Legislative Framework

- Keeping Children Safe in Education (KCSIE) 2025
- Working Together to Safeguard Children
- Teaching Online Safety
- Searching, Screening and Confiscation
- Filtering and Monitoring Standards for Schools and Colleges

- UK GDPR
- Data Protection Act
- Online Safety Act

The school will review this policy annually and immediately following any significant legislative changes, safeguarding updates or serious online safety incidents.

3. Roles and Responsibilities



ROLES & RESPONSIBILITIES IN ONLINE SAFETY



ROLE	KEY RESPONSIBILITIES
 Trustees	• Provide strategic oversight and challenge to ensure effective online safety practices and governance are in place.
 Headteacher	• Ensure online safety is embedded across the school and implemented effectively as part of the school's safeguarding culture.
 DSL	• Lead on online safety and safeguarding. Oversee reporting, risk assessment and support for students affected by online risks.
 Deputy DSLs	• Support the DSL in investigating concerns, managing cases and providing safeguarding support.
 ICT Team	• Manage filtering and monitoring systems, secure the school's network and data, and provide technical support and advice.
 Staff	• Promote safe online behaviour, report any concerns immediately via CPOMS and follow school procedures.
 Students	• Use technology safely, responsibly and respectfully. Report concerns and support others to stay safe online.
 Parents	• Work in partnership with the school to support safe online behaviour at home and engage with guidance and information.


EVERYONE HAS A ROLE

- **EVERY CONCERN MATTERS**
- **TOGETHER WE KEEP STUDENTS SAFE ONLINE**



4. Whole School Approach to Online Safety

Online safety is embedded throughout Newport Girls' High School's safeguarding culture and is recognised as an integral part of child protection. The school acknowledges that technology is a significant factor in many safeguarding concerns and that online risks continue to evolve rapidly. Effective online safeguarding therefore requires a coordinated approach involving leadership, staff, students, parents and external agencies where appropriate.

The school adopts a whole-school approach by:

- embedding online safety within safeguarding, behaviour and pastoral systems
- delivering an age-appropriate online safety curriculum through PSHE, Computing, assemblies and tutor time
- maintaining effective filtering and monitoring systems
- providing regular safeguarding and online safety training for all staff
- engaging parents through newsletters, information evenings and school communications
- responding promptly to emerging online risks and safeguarding concerns
- reviewing incidents to identify trends and improve practice.

Online safety is considered whenever safeguarding concerns are discussed. Staff recognise that abuse may occur both online and offline and that the two are frequently linked.

The school adopts the UK Council for Internet Safety's four categories of online risk:

ONLINE RISK CATEGORIES	
RISK	EXAMPLES
 CONTENT	➤ Exposure to harmful, illegal or inappropriate material including pornography, extremist content, self-harm material, misinformation, AI-generated content and violence.
 CONTACT	➤ Grooming, exploitation, coercion, radicalisation, online fraud, sextortion and inappropriate contact from adults or peers.
 CONDUCT	➤ Cyberbullying, sharing indecent images, harassment, abusive behaviour, online misogyny, trolling, impersonation and unsafe online behaviour.
 COMMERCE	➤ Phishing, scams, gambling, financial exploitation, subscription traps, in-app purchases and cryptocurrency fraud.

The school also recognises that artificial intelligence is creating new safeguarding risks including:

- AI-generated indecent imagery
- deepfakes
- manipulated videos
- AI chatbots encouraging harmful behaviour
- misinformation and disinformation
- identity fraud.

5. Filtering and Monitoring

FILTERING & MONITORING

PROTECT

EDUCATE

EMPOWER

We use a comprehensive filtering and monitoring system to protect students, support staff and maintain a safe digital environment.

OUR SYSTEM

Newport Girls' High School uses Lightspeed Systems to filter, monitor and protect all school devices and school networks.

WEB FILTERING
 Blocks access to inappropriate content based on DfE standards.

REAL-TIME MONITORING
 Monitors online activity to identify potential risks and safeguard students.

SMART ALERTS
 Generates alerts for concerning or harmful online activity.

REPORTING & ANALYTICS
 Provides data and insights to support safeguarding and system effectiveness.

The system is applied to all school-owned devices and school networks, both on site and remotely.

WHO REVIEWS ALERTS?

Alerts are reviewed promptly by trained staff who follow our safeguarding procedures.

DSL TEAM
 The Designated Safeguarding Lead (DSL) and Deputy DSLs review and manage safeguarding alerts.

- ✓ Assess the nature and context of alerts
- ✓ Take appropriate safeguarding action
- ✓ Record and escalate where necessary
- ✓ Liaise with external agencies if required

ICT TEAM
 The ICT team review technical alerts and system issues.

- ✓ Investigate technical faults or breaches
- ✓ Manage system settings and security
- ✓ Ensure filtering is effective and up to date
- ✓ Support data and trend analysis

ANNUAL REVIEW

GOVERNORS
 Filtering and monitoring systems are reviewed annually by the Governing Body.

- ✓ Reviews the effectiveness of filtering and monitoring.
- ✓ Checks compliance with DfE standards and statutory guidance.
- ✓ Evaluates safeguarding impact and emerging risks.
- ✓ Ensures the school's approach continues to be appropriate and proportionate.

Annual review completed by Governors each academic year in the Autumn Term.

OUR KEY PRINCIPLES

SAFETY FIRST
 Protect students from harmful content and online risks.

PROPORTIONATE
 Our systems are appropriate, necessary and balanced.

TRANSPARENT
 We are open about how we filter and monitor.

ACCOUNTABLE
 Clear roles, responsibilities and regular oversight.

SUPPORTIVE
 Monitoring helps us support students, not just protect.

IMPORTANT
 Monitoring is not about spying on users. It is about keeping our students safe, identifying risks early and providing support when needed.
If in doubt – report it.
 Every alert is treated seriously.

6. Managing Online Safety

ONLINE RISKS

Understanding the risks. Knowing our response.

The online world offers many opportunities for learning, connection and creativity, but it also presents risks. We use a consistent, proportionate and safeguarding-focused approach to manage online risks and support all students.

The table below sets out key online risks and the school's response.

RISK	SCHOOL RESPONSE
 Cyberbullying Bullying, harassment or abusive behaviour online.	Managed in accordance with the Anti-Bullying Policy .
 Grooming Adults or peers building relationships to exploit or harm.	Managed in accordance with the Child Protection Policy .
 Sextortion Threats to share intimate images or information.	Immediate referral to the DSL. Managed in accordance with the Child Protection Policy .
 AI abuse The use of AI to create harmful, abusive or inappropriate content.	Managed in accordance with the Behaviour Policy and Child Protection Policy where appropriate.

Our Priority
 We will always act in the best interests of our students and safeguard them from harm online.

ONLINE RISKS (CONTINUED)

RISK	SCHOOL RESPONSE
 Deepfakes AI-generated images, videos or audio used to manipulate or humiliate.	Referred to the DSL for investigation and appropriate action.
 Radicalisation Exposure to extremist ideologies or content that may influence harmful behaviour.	Managed in accordance with Prevent procedures and the Child Protection Policy .
 Self-harm Content or behaviours that promote or encourage self-harm or suicide.	Managed in accordance with the Child Protection Policy and the Mental Health & Emotional Wellbeing Policy .
 Child Criminal Exploitation (CCE) / Child Sexual Exploitation (CSE) Exploitation, coercion or abuse of a child for criminal or sexual purposes.	Managed in accordance with the Child Protection Policy . All concerns will be taken seriously and reported promptly to the DSL.

Key Principles

- ✓ We act early to identify and reduce risks.
- ✓ We provide clear support for students affected by online risks.
- ✓ We work in partnership with parents and external agencies.
- ✓ We review and update our approach regularly.

OUR APPROACH

- ✓ **Education:** Students are taught how to stay safe, responsible and respectful online.
- ✓ **Prevention:** We use technology, policy and practice to limit exposure to risk.
- ✓ **Protection:** We respond quickly to concerns and safeguard all students.
- ✓ **Support:** We provide appropriate support for students, staff and families.
- ✓ **Partnership:** We work with parents, external agencies and the wider community.

Reporting a Concern
 Anyone can report an online concern.
 Report immediately to the DSL via CPOMS.
 If a student is in **immediate danger**, seek help from a member of staff straight away.

Working Together
 Online safety is everyone's responsibility. By working together, we can help our students enjoy the benefits of the online world while staying safe from harm.

Related Policies

- Child Protection & Safeguarding Policy
- Prevent Duty Policy
- Anti-Bullying Policy
- Acceptable Use Policy
- Behaviour & Rewards Policy
- Staff Code of Conduct
- Mental Health & Emotional Wellbeing Policy
- ICT Security Policy

8

9

10

7. Responding to Online Safety Concerns

Every member of staff has a responsibility to act immediately if they have concerns regarding a student's online safety.

Concerns should never be dismissed as "just online" behaviour.

Staff should:

- remain calm
- listen carefully
- avoid asking leading questions
- reassure the student appropriately
- never promise confidentiality
- preserve evidence where possible
- avoid viewing indecent images in line with statutory guidance
- report concerns immediately via CPOMS
- speak directly to the DSL where there is immediate risk.

Where there is an immediate risk of harm, staff should contact the DSL without delay rather than waiting for a written record to be completed.

Recording Concerns

All online safeguarding concerns must be recorded on CPOMS before the end of the working day.

Records should include:

- factual account of the concern
- date and time
- names of those involved
- any evidence secured
- actions already taken
- student's wishes where appropriate
- professional judgement.

CPOMS records should be factual, objective and contemporaneous.

Managing Concerns

The DSL will consider:

- level of risk
- immediate safeguarding needs
- whether parents should be informed
- whether devices require securing
- whether Children's Social Care should be contacted
- whether Police involvement is required
- whether CEOP should be notified
- whether Prevent procedures should be followed
- support required for the student
- support required for other students.

The wishes of the child will always be considered alongside the school's safeguarding responsibilities.

Information Sharing

Information relating to online safeguarding concerns will only be shared where it is lawful, proportionate and necessary to safeguard children.

The school will work collaboratively with:

- parents and carers
- Children's Social Care
- Police
- CEOP
- Prevent partners
- Local Authority
- Health services
- other education providers where appropriate.

Learning from Incidents

The DSL will review online safety incidents regularly to identify:

- recurring themes
- emerging safeguarding risks
- curriculum priorities
- staff training needs
- effectiveness of filtering and monitoring
- changes required to school procedures.

Lessons learned will inform future safeguarding practice, curriculum planning and policy review.

8. Online Safeguarding Risks

Newport Girls' High School recognises that safeguarding concerns increasingly occur through digital technologies and that online abuse may take place both within and beyond the school day. Online abuse can occur between children, between adults and children, or through anonymous individuals and organised groups.

All online safeguarding concerns will be managed in accordance with the Child Protection and Safeguarding Policy, Keeping Children Safe in Education (KCSIE) and other relevant safeguarding procedures.

The table below summarises the school's response to the most significant online risks.



8. ONLINE SAFEGUARDING RISKS



Newport Girls' High School recognises that safeguarding concerns increasingly occur through digital technologies and that online abuse may take place both within and beyond the school day.

All online safeguarding concerns will be managed in accordance with the **Child Protection and Safeguarding Policy**, **Keeping Children Safe in Education (KCSIE)** and other relevant safeguarding procedures.

RISK	SCHOOL RESPONSE
Cyberbullying	Managed in accordance with the Anti-Bullying Policy . Where safeguarding concerns exist, the Child Protection Policy will also apply.
Child-on-Child Online Abuse	The school adopts a zero-tolerance approach. All incidents will be managed in accordance with the Child Protection Policy .
Sharing Nudes and Semi-Nudes	Managed in line with current UKCIS guidance . Staff must not copy, save, forward or investigate imagery. Concerns must be reported immediately to the DSL and recorded on CPOMS .
Image-Based Abuse & Sextortion	Immediate referral to the DSL . The DSL will consider safeguarding support, Police and CEOP involvement where appropriate. Victims will be supported throughout.
Artificial Intelligence & Deepfakes	AI-generated abuse, synthetic imagery and manipulated media will be treated as safeguarding concerns. Students will receive education on responsible AI use and reporting concerns.
Online Grooming	Staff should remain professionally curious regarding changes in behaviour, secrecy or online relationships. All concerns must be reported immediately to the DSL .
Child Sexual Exploitation (CSE)	Managed in accordance with the Child Protection Policy .
Child Criminal Exploitation (CCE)	Managed in accordance with the Child Protection Policy .
Radicalisation & Extremism	Managed in accordance with the school's Prevent procedures and Child Protection Policy .
Online Misogyny & Violence Against Women and Girls	Challenged through the curriculum, Behaviour Policy and safeguarding procedures. Students are taught respectful relationships, consent and equality.
Harmful Online Challenges & Hoaxes	The DSL will risk assess concerns using current DfE and UK Safer Internet Centre guidance before determining an appropriate response.
Online Mental Health Risks	Concerns relating to emotional wellbeing will be managed alongside the Mental Health & Emotional Wellbeing Policy .
Cybercrime	Students will be educated regarding lawful and ethical use of technology. Where appropriate, referrals may be made to the National Crime Agency's Cyber Choices Programme .



STAFF RESPONSIBILITIES

Staff should remain alert to indicators that a student may be at risk online, including changes in behaviour, secrecy, concerning online relationships or distress.



ANY CONCERN, HOWEVER SMALL, MUST BE REPORTED TO THE DSL VIA CPOMS.

Staff Responsibilities

Staff should remain alert to indicators that a student may be at risk online, including:

- significant changes in behaviour or wellbeing
- secrecy regarding online activity
- unexplained gifts or money
- concerning online relationships
- signs of coercion, exploitation or bullying
- distress linked to social media, gaming or messaging platforms.

Any concern, however small, must be reported to the Designated Safeguarding Lead via CPOMS in accordance with the school's Child Protection and Safeguarding Policy.

9. Online Safety Education and Curriculum

Newport Girls' High School recognises that educating students is the most effective way of reducing online risk. The school adopts a progressive, age-appropriate online safety curriculum that develops students' knowledge, skills and confidence to navigate an increasingly complex digital world safely and responsibly.

Online safety education is delivered through a combination of:

- Personal, Social, Health and Economic (PSHE) education
- Computing
- Relationships, Sex and Health Education (RSHE)
- Tutor Time
- Assemblies

- External speakers and workshops
- Safer Internet Day
- National awareness campaigns
- Targeted interventions where specific risks are identified.

Online safety is taught throughout Years 7–13 and reflects current safeguarding trends, student need and national guidance.

Students are taught to:

- recognise online risks
- evaluate the reliability of online information
- understand the impact of their digital footprint
- recognise online manipulation
- use technology responsibly
- protect personal information
- report concerns confidently
- challenge harmful online behaviour safely
- understand the legal consequences of online behaviour
- use artificial intelligence responsibly and ethically.

Teaching will be regularly reviewed to ensure it reflects emerging technologies, current safeguarding concerns and the experiences of Newport Girls' High School students.

Supporting Vulnerable Students

The school recognises that some students may be more vulnerable to online harm.

Additional support may be provided for:

- students with SEND
- looked after and previously looked after children
- students with social, emotional or mental health needs
- students experiencing mental health difficulties
- students who have experienced abuse
- students subject to Child Protection or Child in Need Plans
- students vulnerable to exploitation or radicalisation.

Where appropriate, online safety education will be personalised to meet individual need.

Student Voice

Student views play an important role in shaping the school's online safety provision.

The school will:

- seek student feedback
- monitor emerging online trends amongst young people
- use safeguarding information to inform curriculum planning
- adapt teaching in response to local and national concerns.

Students are encouraged to contribute positively to creating a respectful digital culture across the school community.

10. Artificial Intelligence (AI)

Newport Girls' High School recognises that Artificial Intelligence (AI) is becoming an increasingly important part of education and everyday life. Whilst AI offers significant opportunities to enhance teaching and learning, it also presents safeguarding, ethical and academic risks.

The school is committed to ensuring that students develop the knowledge and critical thinking skills needed to use AI safely, responsibly and ethically.

Student Use of AI

Students may use AI tools where authorised by staff to support learning, for example:

- revision and retrieval practice
- generating ideas
- planning and improving written work
- language translation
- coding support
- accessibility tools.

Students remain responsible for the accuracy, originality and integrity of all work submitted.

AI must not be used to:

- gain an unfair advantage in assessments
- create or share harmful, abusive or inappropriate content
- generate indecent images or deepfakes
- impersonate another person
- bully, harass or intimidate others
- deliberately spread misinformation
- bypass school safeguarding or network security systems.

Misuse of AI will be managed in accordance with the Behaviour Policy and, where appropriate, the Child Protection and Safeguarding Policy.

Staff Use of AI

Staff may use approved AI tools to support planning, administration and teaching, provided they do so professionally, securely and in accordance with school guidance.

Staff must not enter confidential, personal or safeguarding information into AI platforms.

All AI-generated content remains the professional responsibility of the member of staff and should be checked for:

- accuracy
- bias
- appropriateness
- copyright
- safeguarding implications.

Deepfakes and AI-Generated Media

Students will be taught to recognise manipulated media, understand the risks associated with AI-generated content and report concerns immediately.

Any AI-generated abuse, including deepfakes, synthetic imagery or impersonation, will be treated as a safeguarding concern and managed in accordance with the school's safeguarding procedures.

11. Staff Professional Conduct Online

All staff have a responsibility to model safe, respectful and professional online behaviour.

Professional conduct applies equally within and outside working hours where behaviour could affect professional reputation or the safety of students.

Staff must:

- maintain appropriate professional boundaries
- use school systems appropriately
- protect confidential information
- follow the Staff Code of Conduct
- comply with data protection legislation
- report safeguarding concerns immediately
- maintain secure passwords and multi-factor authentication where available.

Social Media

Staff should exercise professional judgement when using social media.

Staff must not:

- communicate privately with students using personal accounts
- accept friend requests from current students
- share confidential information
- post material that could undermine public confidence in the school
- discuss safeguarding matters online
- identify students without permission.

School communication with students will only take place through authorised school systems.

Photography and Recording

Images or recordings of students may only be taken using authorised school equipment.

Staff must never:

- use personal mobile phones to photograph students
- store student images on personal devices
- upload student images to personal cloud storage
- share images via personal messaging services.

Images will only be used in accordance with parental consent and data protection requirements.

I2. Mobile Phones, Smart Watches and Personal Electronic Devices

The use of mobile phones, smart watches and personal electronic devices is managed through the Behaviour Policy. Students are expected to comply with these expectations at all times. Any misuse of technology will be managed in accordance with the Behaviour Policy and safeguarding procedures where appropriate.

I3. Cyber Security

Newport Girls' High School recognises that effective cyber security is fundamental to safeguarding, protecting personal data and ensuring continuity of education.

The school will maintain appropriate technical and organisational measures to protect its network, systems and users from cyber threats.

Cyber security arrangements are aligned with the **National Cyber Security Centre (NCSC)** guidance and the **DfE Digital and Technology Standards**.

Network Security

The ICT Team will ensure that:

- firewalls remain active and are regularly reviewed
- anti-virus and anti-malware software are kept up to date
- operating systems receive security updates promptly
- security patches are applied without unnecessary delay
- user accounts are appropriately managed
- administrator privileges are restricted
- network access is appropriately controlled
- secure back-up arrangements are maintained
- remote access is protected through secure authentication
- appropriate audit logs are retained.

Regular vulnerability testing and system reviews will be undertaken to minimise cyber security risks.

Password Security

All users are responsible for maintaining secure passwords.

Passwords should:

- be unique
- contain an appropriate combination of letters, numbers and symbols
- never be shared
- never be written where they can be accessed by others
- be changed immediately if compromise is suspected.

Where available, multi-factor authentication (MFA) will be enabled to strengthen account security.

Staff must never share login credentials or allow others to access systems using their accounts.

Phishing and Email Security

Cyber criminals increasingly target schools through phishing emails and malicious links.

Staff and students will be trained to recognise:

- suspicious email addresses
- unexpected attachments
- fake login pages
- QR code scams
- requests for passwords
- requests for financial information
- urgent or threatening language
- suspicious hyperlinks.

Any suspected phishing email must be reported immediately to the ICT Team.

Staff must never:

- open suspicious attachments
- provide passwords via email
- transfer money following an email request without verification
- enter school credentials into unknown websites.

Data Protection

All staff are responsible for protecting personal information.

Confidential information must only be stored:

- on approved school systems
- using secure storage
- in accordance with the Data Protection Policy.

Personal information must never be uploaded to unauthorised websites or AI platforms.

Any suspected data breach must be reported immediately to the Headteacher, DSL and Data Protection Lead.

Cyber Incidents

Where a cyber incident occurs, the school will:

- contain the incident
- preserve evidence
- notify relevant senior leaders
- assess safeguarding implications
- restore systems safely
- report incidents where required
- review lessons learned.

Where appropriate, advice will be sought from:

- National Cyber Security Centre
- Local Authority
- Police
- Department for Education
- Information Commissioner's Office.

14. Acceptable Use of Technology

All members of the school community are expected to use technology responsibly, safely and respectfully.

Separate Acceptable Use Agreements are issued for:

- students
- staff
- governors
- visitors where appropriate.

These agreements are reviewed annually.

Failure to comply may result in:

- behaviour sanctions
- disciplinary procedures
- withdrawal of access
- safeguarding referrals
- Police involvement where criminal offences may have occurred.

15. Partnership with Parents and Carers

Parents will receive regular online safety updates through newsletters, information evenings and school communications.

Supporting Safe Technology Use at Home

The school encourages parents to:

- keep devices updated
- use parental controls where appropriate
- supervise younger children's online activity
- encourage balanced screen time
- discuss online friendships
- talk openly about online risks
- encourage children to report anything that makes them feel uncomfortable.

The school recognises that open communication between home and school is one of the strongest protective factors in keeping children safe online.

16. Monitoring, Evaluation and Quality Assurance

Online safety arrangements will be monitored continuously throughout the academic year.

The DSL will identify trends and recommend improvements where necessary.

17. Policy Review

This policy will be reviewed:

- annually
- following significant safeguarding incidents
- following changes to statutory guidance
- following significant developments in technology
- where internal review identifies the need for amendment.

Minor operational changes may be approved by the Headteacher and Designated Safeguarding Lead between formal review dates.

